Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 2 of 20

AMENDMENTS TO THE CLAIMS

1. (CURRENTLY AMENDED)   An image encrypting method, comprising:

a first process of inputting an image by reading an image file expressing the image;

a second process of dividing said image file into portion image data of a predetermined unit;

a third process of generating information incidental to said portion image data, said incidental information including boundary information which expresses a boundary dividing respective said portion image data; and

a fourth process of encrypting every said portion image data to provide every said portion image data with security so that unauthorized access to the portion image data cannot be obtained without decrypting,

wherein image-handling of said portion image data is performed by using said incidental information ~~and~~ so that the image-handling is performed while said portion image data remains encrypted ~~during the image-handling~~.

2. (PREVIOUSLY PRESENTED) The image encrypting method according to claim 1, further comprising: a fifth process of generating an encrypted image file from encrypted portion image data generated in said fourth process and said incidental information generated in said third process.

Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 3 of 20

3. (PREVIOUSLY PRESENTED) The image encrypting method according to claim 2, wherein said encrypted image file includes a plurality of marking means, each of said marking means being attached to respective said encrypted portion image data so as to identify respective boundaries between said encrypted portion image data in said encrypted image file.

4. (PREVIOUSLY PRESENTED) The image encrypting method according to claim 1, wherein said incidental information is encrypted, and an encrypted image file including encrypted portion image data and encrypted incidental information is generated in said fourth process.

5. (PREVIOUSLY PRESENTED) The image encrypting method according to claim 4, wherein said incidental information includes each position information of respective said encrypted portion image data in said encrypted image file and each size information of respective said encrypted portion image data.

6. (CURRENTLY AMENDED)   An image encrypting device, comprising:

inputting means which inputs an image by reading an image file expressing the image;

Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 4 of 20

image portion unit dividing means which divides said image file into portion image data of a predetermined unit;

encrypting means which encrypts every said portion image data to provide every said portion image data with security so that unauthorized access to said portion image data cannot be obtained without decryption;

identifier generating means which generates information incidental to said portion image data, said incidental information which expresses a boundary dividing respective said portion image data; and

file generating means which generates an image file on the basis of said portion image data encrypted by said encrypting means and said incidental information generated by said identifier generating means,

wherein image-handling of said portion image data is performed by using said incidental information ~~and~~ so that the image-handling is performed while said portion image data remains encrypted ~~during the image-handling~~.

7. (PREVIOUSLY PRESENTED) The image encrypting device according to claim 6, wherein the image file generated by said generating means is an encrypted image file.

Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 5 of 20

8. (PREVIOUSLY PRESENTED)   The image encrypting device according to claim 7, wherein said encrypted image file includes a plurality of marking means, each of said marking means being attached to respective encrypted portion image data so as to identify respective boundaries between said encrypted portion image data in said encrypted image file.

9. (PREVIOUSLY PRESENTED) The image encrypting device according to claim 6, wherein said encrypting means encrypts said incidental information, and said file generating means generates the image file on the basis of said portion image data encrypted by said encrypting means and said incidental information encrypted by said encrypting means.

10. (PREVIOUSLY PRESENTED)   The image encrypting device according to claim 9, wherein said incidental information includes each position information of respective encrypted portion image data in said encrypted image file and each size information of respective encrypted portion image data.

11. (CURRENTLY AMENDED)   A recording medium on which are recorded image encrypting procedures, comprising:

a first step of inputting an image by reading an image file expressing the image;

Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 6 of 20

a second step of dividing said image file into portion image data of a predetermined unit;

a third step of generating information incidental to said portion image data, said incidental information including boundary information which expresses a boundary dividing respective said portion image data;

a fourth step of encrypting every said portion image data to provide every said portion image data with security so that unauthorized access to the portion image data cannot be obtained without decryption; and

a fifth step of image-handling said portion image data by using said incidental information, wherein information so that the image-handling is performed while said portion image data remains encrypted during the image-handling.

12. (PREVIOUSLY PRESENTED)   The recording medium on which are recorded image encrypting procedures according to claim 11, further comprising: a sixth step of generating an encrypted image file from encrypted portion image data generated in said fourth step and said incidental information generated in said third step.

13. (PREVIOUSLY PRESENTED)   The recording medium on which are recorded image encrypting procedures according to claim 12, wherein said encrypted

Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 7 of 20

image file includes a plurality of marking means, each of said marking means being attached to respective said encrypted portion image data so as to identify respective boundaries between said encrypted portion image data in said encrypted image file.

14. (PREVIOUSLY PRESENTED)   The recording medium on which are recorded image encrypting procedures according to claim 11, wherein said incidental information is encrypted, and an encrypted image file including encrypted portion image data and encrypted incidental information is generated in said fourth step.

15. (PREVIOUSLY PRESENTED)   The recording medium on which are recorded image encrypting procedures according to claim 14, wherein said incidental information includes each position information of respective said encrypted portion image data in said encrypted image file and each size information of respective said encrypted portion image data.

16.   (CURRENTLY AMENDED)   A recording medium on which an encrypted image file is recorded, said encrypted image file being generated by:

a first process of inputting an image by reading an image file expressing the image;

Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 8 of 20

a second process of dividing said image file into portion image data of a predetermined unit;

a third process of generating information incidental to said portion image data, said incidental information including boundary information which expresses a boundary dividing respective said portion image data; and

a fourth process of encrypting, per predetermined unit, every said portion image data which has been divided into said predetermined unit to provide every said portion image data with security so that unauthorized access to said portion image data cannot be obtained without decryption,

a fifth process of image-handling said portion image data by using said incidental ~~information,~~ ~~wherein~~ information so that the image-handling is performed while said portion image data remains encrypted ~~during the image-handling~~.

17. (PREVIOUSLY PRESENTED)   The recording medium on which an encrypted image file is recorded according to claim 16, said encrypted image file being generated by a fifth process of generating said encrypted image file from encrypted portion image data generated in said fourth process and said incidental information generated in said third process.

Docket No. 1982-0137P
Appl. No.: 09/400,297
Art Unit: 2175
Amendment dated November 16, 2004
Reply to Office Action of May 19, 2004
Page 9 of 20

18. (PREVIOUSLY PRESENTED)   The recording medium on which an encrypted image file is recorded according to claim 17, wherein said encrypted image file includes a plurality of marking means, each of said marking means being attached to respective said encrypted portion image data so as to identify respective boundaries between said encrypted portion image data in said encrypted image file.

19. (PREVIOUSLY PRESENTED)   The recording medium on which an encrypted image file is recorded according to claim 16, wherein said incidental information is encrypted, and said encrypted image file including encrypted portion image data and encrypted incidental information is generated in said fourth process.

20. (PREVIOUSLY PRESENTED)   The recording medium on which an encrypted image file is recorded according to claim 19, wherein said incidental information includes each position information of respective said encrypted portion image data in said encrypted image file and each size information of respective said encrypted portion image data.